UNITED STATES DISTRICT COURT

DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	C.A. 1:12-md-02358-ER

This Document Relates to:
All Actions

DECLARATION OF LAWRENCE YOU

I, Lawrence You, declare and state as follows:

Introduction

1. I am the Director of Privacy for Product and Engineering, and a member of the Engineering team at Google LLC ("Google"). I am the designated corporate declarant for Google regarding the matters set forth herein, of which I have personal knowledge and/or belief, and, if called as a witness, I could and would testify competently thereto.

2. I understand that the plaintiffs in this action ("Plaintiffs") allege that they used the Apple Safari and/or Internet Explorer web browsers to visit websites on which Google and other defendants displayed advertisements, and that when Google showed them advertisements, Google may have placed "cookies" on their browsers even though their browsers' settings allegedly suggested that such cookies would be blocked.

3. In this declaration, I will explain the following facts:

   a. The substantial majority of persons upon whose behalf this action was filed were not affected by the placement of the cookies in the manner alleged by Plaintiffs because they already had the cookie at issue on their browser for reasons unconnected with the events alleged by Plaintiffs.

   b. Because the cookie itself gives no indication of how it was placed, it is not possible for Google, Plaintiffs, or members of the class of persons represented by Plaintiffs to identify whether a browser received a cookie by the means alleged by Plaintiffs or by some other means not at issue. Google did not collect and does not have information sufficient to identify the class of persons whose browsers received a cookie by the means alleged by Plaintiffs.

c. If a cookie was placed in the manner alleged by Plaintiffs, the only result would have been the possibility that more relevant ads (interest-based advertising) might have been displayed rather than the less relevant ads otherwise displayed on a particular website (context-based advertising).

4. Understanding these facts requires some background in how Internet advertising worked and how cookies were used during the relevant time period (late 2011 to early 2012). Although I speak in the present tense, the statements herein refer to 2011 Internet browsing technology and may no longer be accurate for present-day Internet browsing technology.

How Internet Browsing Works

(During the relevant time period in 2011)

5. For the most part, devices connected to the Internet can be divided into "servers", being the devices on which content is hosted, and "clients", being devices such as laptops and smartphones on which the content is received and viewed. Every website is hosted on a server.

6. Every device that connects to the Internet has an Internet Protocol ("IP") address. An IP address is a sequence of numbers which identifies the point at which a particular device is connected to the Internet.

7. A website address (also known as a uniform resource locator or "URL"), such as www.uscourts.gov, is associated with the particular IP address of the server on which the website is hosted.

8. In order to view the content appearing at a specific URL, most Internet users use a web browser (or browser). A web browser is a software application (i.e., a type of computer program) which is installed on a user's device, whether a desktop PC, a laptop, a tablet or a smartphone. The purpose of a browser is to request content from websites and to interpret the format of the

content received in response to a request, so that it is correctly displayed on the device. There are a number of different browsers available, such as Microsoft's Internet Explorer, Google's Chrome, Mozilla's Firefox and Apple's Safari. These may differ in respect of their appearance and functionality. An individual device may have a number of different browsers installed on it.

9. A user wanting to access a particular website can either type the web address in the address bar in his/her browser or click on a hyperlink from another page, such as an entry in a list of search engine results or a post on a social network. At this point, the browser sends a request to a domain name server. These are extensive databases, forming the Domain Name System (DNS), which perform a similar function to a telephone directory, by linking the web addresses to the IP addresses of the servers on which the websites are hosted. When a domain name server makes a match, it will direct the browser's request to the server on which the website is hosted.

10. When a browser sends a request to a website's server, it includes certain information generated by the browser as part of the request. This includes the IP address that the user's device is connected through, so that the server knows to which device the requested content is to be sent. The server on which a website is hosted receives the browser request and sends the requested content back to the browser via the IP address transmitted as part of the request. The transmission of content in this way is often referred to as "serving" a web page. The browser accepts the content received, and displays the web page to the user.

11. Many modern websites include content from multiple sources. In such cases, the website content is served from different servers made available by multiple parties. For example, a news publisher may partner with a weather publisher, so that its news website displays "news content" from the news publisher's own server alongside "weather content" from the weather publisher's

server. When the browser sends the initial request to the "main" website's server (i.e. the news publisher's server), the server will respond by sending the news content to the browser along with instructions telling the browser where to get the weather content. The browser will then make an additional request to the weather publisher's server.

Websites with Advertising Content

(During the relevant time period in 2011)

12. Many website publishers lease out space on their web pages for advertising purposes. The website publisher will make a section of space on a web page (such as a rectangular "banner") available for an advertiser to display an advertisement. The serving of third-party advertising content (often referred to as "ad-serving") is accomplished in the same way as described above, typically from an "ad server" operated by an advertising services provider (or "ad-network"). Thus what appears on a user's device as a single web page will often be comprised of content, including advertisements, from multiple different domains, hosted on different servers.

13. As with the request to the main website, when a browser is directed to request content from additional servers, such as an ad server, the browser will include information generated by the browser as part of the request.

14. As I will explain in more detail, one aspect of Google's business is to provide advertising services for website publishers. Google operated some such services, for example its "AdSense" program, from the doubleclick.net domain.

Information Communicated by the Browser

(During the relevant time period in 2011)

15. As explained above, in order to view content online, the user's browser will send a request to the server hosting the requested content. The browser's request contains various pieces of

information, including the type of browser, the operating system of the device, the screen resolution of the device and the IP address of the device on which the browser is running ("Browser-Generated Information"). Among other things, Browser-Generated Information ensures that content can be delivered to, and properly displayed on, the browser of the device in question. The exchange of Browser-Generated Information in this way is standard and fundamental to the technical operations which enable users to browse the Internet.

16. Browser-Generated Information will be communicated by a browser to any server from which content is requested, every time the browser sends such a request. Where a web page is made up of content from different sources (or domains), the Browser Generated Information will be transmitted to each of the sources (or domains) that is providing it. The Browser-Generated Information sent to such other content sources may also include the URL of the "main" website which the browser is displaying.

The Setting of Cookies

(During the relevant time period in 2011)

17. Most websites use cookies. A cookie is a small string of text which can be stored on the user's device. When a website's server responds to a request from a browser, the server may also request that a cookie be stored (or "set") on the device from which the browser's request was sent.

18. Cookies can be used in a variety of ways. One way in which a cookie can be used is as a unique identifier to help a website recognize returning visits by the same browser on a particular device on different occasions. For example, a shopping website with "add to basket" functionality may use cookies to recognize that it is the same browser moving from page to page, so that the contents of the basket can be retained. To give another example, a website that requires users to

log in (e.g., a newspaper site which requires a subscription) may use cookies to recognize a user's browser and enable the user to access the website without needing to reenter his or her login details. Cookies may also have associated values, for example they may include the date on which the cookie was set and/or the period after which the cookie is to expire.

19. To use a cookie as a unique identifier, the cookie needs to be set with a unique ID in the form of a string of characters unique to that cookie. The browser sends a request to the server which hosts the website. The server sends back the requested content and (unless the cookie is already present on the user's browser) requests that a cookie be stored.

20. If the cookie is set on the user's browser, then (until the cookie expires or is deleted) the browser will include the cookie along with the Browser-Generated Information in any future content requests it sends to that particular website (or domain). A cookie can only be read by the website (or domain) that set it.

Cookies Set by Advertising Networks such as Google's DoubleClick

(During the relevant time period in 2011)

21. As explained above, where a web page is made up of content from different sources (or domains), for example where the web page includes third-party advertising content, the browser will need to send a request to both the server on which the "main" content is hosted, and then to the ad server on which the advertising content is hosted. When the ad server responds with the relevant content, it may request that a cookie be set on the user's browser. The cookie that is set may contain a unique ID. If a cookie with a unique ID is set, the relevant ad network will be able to recognize the particular browser again if they interact in the future. This is the purpose of Google's "DoubleClick Ad Cookie" which typically (but not always) includes a unique ID.

22. By correlating the unique ID of a DoubleClick Ad Cookie with the Browser Generated Information received over time from the browser on which the DoubleClick Ad Cookie is set, Google can maintain a record of some of the Google ad websites that a particular browser has visited over time. This allows Google to serve interest-based advertising better tailored to that browser as a result (for example, it may serve motorcycle ads to a browser that has visited multiple websites about motorcycles).

23. It is important to understand, however, that (i) only Google's servers hosting the DoubleClick domain (doubleclick.net) are able to read a DoubleClick Ad Cookie; and (ii) Google will only be provided with the Browser-Generated Information when the browser's request is directed to the DoubleClick domain. This means that the information which Google receives will only relate to those websites that participate in Google's DoubleClick advertising services. Accordingly, the correlation undertaken by Google using the DoubleClick Ad Cookie will represent only a part of the online activity of a particular browser.

24. It is also important to note that the DoubleClick Ad Cookie does not itself collect or contain any information about the user or the browser, nor does it cause the Browser Generated Information to be sent. As explained above, the DoubleClick Ad Cookie contains an anonymous cookie value in the form of a string of characters unique to that cookie. When correlated with a DoubleClick Ad Cookie ID, the Browser-Generated Information does not identify an individual (as it simply relates to a browser running on a device). Further, at the relevant time, it was Google's practice that Browser Generated Information correlated with a DoubleClick Ad Cookie ID was not associated with any user data in Google's possession (for example, it was segregated from the account data that resided in Google accounts used to access Gmail, YouTube and other Google services).

25. It is also important to note that it is possible to "block" the setting of a cookie. Cookies, including the DoubleClick Ad Cookie, will only be set on a browser if the browser's settings allow it to accept cookies. I will return to this point later.

"Opting-out" of Interest-Based Advertising

(During the relevant time period in 2011)

Google's "Ads Preference Manager"

26. Users who do not want Google to collate Browser-Generated Information have different means of "Opting-out." One means by which users can opt-out is via Google's "Ads Settings" page (previously called "Ads Preference Manager"), where users can click to opt-out of receiving interest-based advertising from Google. If a user selects "opt-out", the DoubleClick Ad Cookie is set (or overwritten) with the value "OPT_OUT" (i.e., it does not contain a unique ID). This means that the DoubleClick domain will still receive the same Browser-Generated Information from the browser as part of the request, but it will be unable to correlate that information with a unique ID, and it will be unable to distinguish one opted-out browser from another. Consequently, Google cannot use the DoubleClick Ad Cookie to serve interest-based advertising to browsers whose users have opted out in this way. This option is available to all Internet users, via Google's websites, regardless of the browser they use (and was available to users throughout the period relevant to this claim).

Blocking "Third-Party" Cookies

27. As explained earlier in this statement, a browser's settings can also be used to manage how and when it will receive cookies. The browser's developers establish the circumstances in which their browser's specific cookie-blocking settings will either accept or block cookies. Major browsers, including Safari, include options that allow users to block what are commonly referred

to as "first-party" cookies (i.e., those from the first or "main" website which the browser is requesting content from, for example the news website's server as described above) and/or "third-party" cookies (i.e., those not from the "main" website, for example the weather publisher's server as described above).

28. Whether a cookie is considered a first or third-party cookie is determined by the context in which it is set, and not by the cookie itself. Cookies are set as a result of an interaction between a browser and a server, as described above. Like most advertising cookies, Google's DoubleClick Ad Cookie can be set either on a first or third-party basis. Google has no way of telling whether any individual DoubleClick Ad Cookie has been set on a first- or third-party basis. I will return to this point later.

Setting "First-Party" Cookies

29. A browser which is set to reject third-party cookies can still receive a DoubleClick Ad Cookie if it interacts with the DoubleClick domain on a first-party basis. This will typically occur when a user clicks on an advertisement served by DoubleClick, since the browser's request will be directed to the DoubleClick domain before it reaches the advertiser's site. (This is the way most ad networks operate; it is an important step in attributing a "clickthrough" (i.e. a user's interaction) to the particular advertisement that was served.) Consequently, in this scenario, the DoubleClick domain's request to set a cookie would be on a first-party basis. As this would not be a third-party cookie, it would not be rejected by a browser set to reject third-party cookies. The user could, however, block the DoubleClick Ad Cookie entirely by changing his/her browser settings to reject cookies set on both a first- and third-party basis. This option was available on Safari, throughout the period relevant to this claim.

Google+ and Social Ads

30. In order to properly understand the background to this claim, it is necessary for me now to explain a Google initiative relating to Google+ users and social ads. Google+ is a social network provided by Google, launched in June 2011. It allows its users to connect with other Google+ users, follow other users to see what they are sharing, and group their connections into "Circles", for example "family" or "art lovers." Users can post photographs, status updates and other content, and share this publicly to their stream, or just to specific Circles or interest-based communities. To use Google+ it is necessary to have a Google account, which involves users providing information about themselves, such as their name.

31. Google developed a new feature to enable advertisements served by the DoubleClick domain to be tailored to the social connections of users of Google+. This feature was launched in October 2011 and was only available to Google+ users who consented to it. It enabled logged-in Google+ users to highlight (or "+1") Google advertisements they liked, and to be served advertisements that their social connections liked. Instead of simply seeing an advertisement served by the DoubleClick domain when browsing the Internet, the advertisement would be overlaid with a banner at the foot of the advertisement that identified which of those user's social connections had liked (or "+1'ed") that advertisement. Such advertisements were known as "social ads."

32. I have already explained Google's approach to keeping DoubleClick data segregated from Google account data. However, in order to offer social ads, the DoubleClick domain needed to be able to identify whether a user was logged in to Google+ and had opted-in to social ads, and to have access to information about who their social connections were and which advertisements their social connections "+1'ed." However, at the same time, Google wanted to ensure that, in

facilitating this, personal Google account information provided by users would not be associated with information obtained via the DoubleClick Ad Cookie, since such association could compromise the anonymity of the DoubleClick Ad Cookie. In other words, Google needed to be able to identify the specific advertisements that social connections of an individual Google+ user had "+1'ed", while ensuring that it continued to segregate Google account information and DoubleClick Ad Cookie information.

The Intermediary Cookie

33. Google therefore designed what I will refer to as the intermediary cookie to act as a temporary encrypted intermediary between the two distinct account and advertising systems. Its purpose was to control DoubleClick's access to Google account data. To achieve this, Google designed the intermediary cookie in such a way that only limited, encrypted data was provided to Google's DoubleClick systems. This ensured that the DoubleClick systems could not access the user's personal account information. The intermediary cookie did not collect any personal information and was not used to correlate Browser-Generated Information. The intermediary cookie therefore allowed the DoubleClick domain to show relevant Google+ users (those who had consented to social ads) which of their Google+ connections (who had also consented to social ads) had "+1'ed" that particular advertisement, while ensuring that DoubleClick could not access personal Google account data.

34. Following implementation of the intermediary cookie, when any browser (Internet Explorer, Chrome, Firefox, Safari, etc.) interacted with a website that was participating in Google's DoubleClick advertising services, the DoubleClick domain would seek to set the intermediary cookie in one of three cases:

a. Where the user was logged in to their Google account and they had opted-in to seeing social ads. In this case, the intermediary cookie would be set to contain the user's encrypted account identifier;

b. Where the user was not logged in to a Google account (either because they were logged out or because they did not have a Google account). In this case, the intermediary cookie would be set in an inert form, containing only a "No Data" value and no unique ID. This effectively served as a "do not disturb" mechanism; and

c. Where the user was logged in but had opted-out of seeing social ads, the intermediary cookie would again be set in an inert form, containing only an "opt-out" value and no unique ID. Again, the intermediary cookie served as a "do not disturb" mechanism.

35. The "No Data" and "opt-out" versions of the intermediary cookie reduced latency. The term "latency" refers to the delay before a transfer of data begins, following an instruction for its transfer. Setting a "No Data" / "opt-out" version of the intermediary cookie avoided multiple interactions between those browsers and the DoubleClick server. It meant that the intermediary cookie could be sent to the DoubleClick server at the same time as the Browser-Generated Information, as described earlier in this statement, so that the DoubleClick server did not need to make further enquiries of the browser to establish whether it was logged in to the user's Google Account or whether the user had opted-in to social ads.

36. Prior to launching the social ads feature, Google tested social ads on Safari. This was to ensure that the setting of the intermediary cookie did not have an adverse impact on the performance of DoubleClick Ad Cookies which had already been set. It is common practice to test product enhancements on an incremental basis like this. In connection with those early tests, the intermediary cookie was only set on browsers that already had a DoubleClick Ad Cookie

present on them. The intermediary cookie was launched globally on September 20, 2011 and social ads was launched in October 2011.

37. I have explained that the intermediary cookie was designed to control DoubleClick's access to Google account data. I should make it clear that the intermediary cookie was effective in meeting this objective. The difficulties with the intermediary cookie which I will describe were not the result of any failures in this regard.

Apple's Safari Browser

(During the relevant time period in 2011)

38. Safari, developed by Apple Inc., is the default browser installed on Apple computers, iPhones and iPads. Unlike other major browsers, Safari's default settings generally disallow third-party cookies. Although many other browsers offer this functionality, it is not normally the default setting, as the blocking of such cookies can disrupt the features of many modern websites, resulting in a poor experience for users. For instance, sites like Facebook operate platforms that host third-party applications including games and media players. Those applications could not recognize returning users or remember users' preferences if they could not set third-party cookies. These usability problems were a particular issue for users of Safari, given Safari's default setting.

39. Over time, Apple developed exceptions to Safari's default settings to address the concern that its default blocking of third-party cookies caused usability problems. Two of these exceptions are relevant here and explained below.

40. One such exception was known as the "HTML Form Submission" method: if a request to a third-party domain was generated by the submission of a HTML form, Safari allowed the response to that request to set a cookie. Over time, this approach became known to web

developers. It was reflected in Facebook's "Best Practices" Guide for Developers, which briefly describes this difficulty with Safari and links to a blog post written by a programmer called Anant Garg containing instructions on how to implement a "solution" using the "HTML Form Submission" method.

41. Since the setting of the intermediary cookie would take place on a third-party basis, it would typically be blocked by Safari, by default. Consequently, Google would have been unable to implement social ads for users of Safari browsers who consented to receiving them, unless those users changed the default Safari settings. To solve this problem, Google used known Safari functionality, the "HTML Form Submission" method, to set the intermediary cookie on relevant Safari browsers. The "HTML Form Submission" method did not require the user to change their default settings in order for it to be effective.

42. In addition to the "HTML Form Submission" exception, it is now clear that Apple's engineers had developed other exceptions to its settings, no doubt due to the various problems that Safari's default blocking of third-party cookies caused. For example, Safari's blocking of third-party cookies interfered with many popular web functionalities, such as social "like" buttons, used to integrate third-party social features into websites.

43. One such exception, now known as the "One In, All In" exception, involved Apple relaxing Safari's approach to allow all cookies to be set from a third-party domain if a cookie from that domain was already present on the browser. This approach to cookies was unique to Safari among major web browsers and it was only implemented for certain versions of Safari (5.0 and above) and only on certain versions of Apple's iPhone operating systems (iOS version 4.1.2 and above).

44. As I have explained above, Google's intermediary cookie was designed to be set by the DoubleClick domain, in order to provide social ads to Google+ users who had consented to them. As a result of the "One In, All In" exception, Safari browsers on which an intermediary cookie was set (including in an "Opt Out" or "No Data" form, as described above) would then also accept a DoubleClick Ad Cookie, on a third-party basis, in spite of Safari's default settings. This was because the DoubleClick Ad Cookie was also set by the same DoubleClick domain.

45. Safari users who received the DoubleClick Ad Cookie as a result of the "One In, All In" exception could have seen interest-based advertisements which were more tailored than they otherwise would have been. In effect, these users saw the same type of interest-based advertising that they would have seen had they been using any other major browser in its default setting.

46. In addition to exceptions which Apple specifically developed to avoid the operation of Safari's default settings, those default settings were not always effective for other reasons. It is likely that many cookies (including DoubleClick Ad Cookies) were set as a result of technical bugs in Safari's cookie handling mechanisms, causing Safari browsers to accept third-party cookies even where they were set to reject them. For example, it has been reported that:

a. for a period of time, when using "Private Browsing" mode, Safari browsers accepted cookies even when a user's cookie blocking settings were set to "Always";

b. when Apple introduced Safari version 5.1 as part of its "Lion" operating system upgrade, some users reported that Safari browsers were no longer blocking cookies regardless of their browser settings.

Removal of the DoubleClick Ad Cookies from Safari Browsers

47. Prompted by external enquiries in February 2012, Google took technical steps to address the side-effects that resulted from setting the intermediary cookie on versions of Safari with "One

In, All In". Google stopped DoubleClick's servers from sending requests to set the intermediary cookie using the "HTML Form Submission" method and also began expiring all intermediary and DoubleClick Ad Cookies on Safari browsers.

It Is Impossible to Identify Individually Those Who Were Affected

48. To recap, I have explained how the matters that form the basis of the complaint were the result of the combination of (i) Google's use of the "HTML Form Submission" method to set intermediary cookies; (ii) the setting of the intermediary cookie taking place from the DoubleClick domain; and (iii) Apple's introduction of the "One In, All In" exception. Only a small portion of Safari users were actually affected by the combination of these factors. And it is impossible to identify individually those who were affected.

49. DoubleClick Ad Cookies are created without prior association to users, meaning, the content of the cookie itself has no association with a user's identity or other personally identifying information. The string of alphanumeric characters that comprise the DoubleClick Ad Cookie is designed to be anonymous and deliberately processed independently of other information such as Google accounts, email addresses, phone numbers, physical address, and other personally identifying information, so as to maintain anonymity.

50. IP addresses by themselves do not identify individuals. A single device can change IP addresses quickly, especially on mobile networks. There can be multiple devices used by a single IP address concurrently, for example with an internet proxy or router. Accordingly, when a browser with a DoubleClick Ad Cookie communicates with Google's servers, the IP address communicated by that browser is not processed as personally identifying information. As with the DoubleClick Ad Cookies, Google processes the IP addresses anonymously and uses the

information to provide improvements to general purpose ads performance such as coarse (and sometimes incorrect) approximation of geographical location and to detect abuse and fraud.

51. When communicating with a browser that has a DoubleClick Ad Cookie, Google's servers by design do not request, nor do they receive, personally identifying information that may have been stored elsewhere in the browser such as saved addresses or email addresses. This is a basic and fundamental security protection that all browsers must provide.

52. As explained above, the DoubleClick Ad Cookie could be set on a first- or third-party basis. However, the matters complained about only affected individuals on whose Safari browser the DoubleClickAd cookie was set on a third-party basis as a result of the combination of factors I have described. Many Safari users would have received the DoubleClick Ad Cookie on a first-party basis prior to the introduction of the intermediary cookie.

53. Google has retained relevant server log information for the purposes of litigation since 2012. It is important to appreciate that this server log information is not entirely complete, contains data unrelated to this litigation and is significantly cumbersome to analyze. Furthermore, Google's server log information is not concerned with the intermediary cookie because Google never recorded relevant information about the intermediary cookie. I will address this point further below.

54. The data is stored across multiple servers and requires very significant storage and computing power (and expertise) to analyze it. Analysis is done by writing custom query scripts using a special software language similar to SQL that facilitates searches of server log information. The query processor is a system for analysis of read-only "nested" data, which runs aggregation queries over tables of many billion rows, across thousands of central processing units and many terabytes of data.

55. I have previously explained that Google does not have any way of telling whether any particular DoubleClick Ad Cookie has been set on a first- or third-party basis. Accordingly, Google had no means of knowing, either at the time the cookies were set, or by analyzing the data it has retained, which specific browsers were affected by the combination of factors I have described (and in particular the "One In, All In" exception which permitted the setting of the DoubleClick Ad Cookie).

56. At best, the existing data can be used to estimate a percentage of Safari browsers that may have received a DoubleClick Ad Cookie because of the "One In, All In" issue described above. Such an estimation cannot be exact. Google has estimated from this data that before relevant testing of the intermediary cookie began in August 2011, the vast majority of Safari browsers already had a DoubleClick Ad Cookie before the event at issue in this action could have had any effect. As I have explained, in these instances the DoubleClick Ad Cookie could have been set on a first-party basis, where the user had clicked on an advertisement served by DoubleClick advertising services, or on a third-party basis, where the browser's settings had been changed to accept third-party cookies. Also, as I have previously mentioned, it is likely that some users would have received the DoubleClick Ad Cookie as a result of technical bugs in Safari's cookie handling mechanism.

57. The vast majority of Safari users were thus unaffected by the "One In, All In" exception. At the end of the relevant time period in February 2012, many Safari browsers still lacked a DoubleClick Ad Cookie. These include browsers that had been set by their users to reject all cookies; browsers that had been set to opt-out of third-party advertising (for example, via Google's Ads Preference Manager or a third-party tool); and browsers that could not have been affected by the "One In, All In" exception, because they had not been upgraded to the latest

version of Safari, or which were running on devices that had not been upgraded to the latest Apple operating system.

58. I have previously explained that the intermediary cookie was designed to act as a temporary encrypted intermediary between the two distinct account and advertising systems to control DoubleClick's access to Google account data. For this reason, the server that handled requests to the URL "/pagead/drt/si" (from which the intermediary cookie was set) did not generate any logs. At the relevant time, where a user wished to opt out of receiving interest-based advertising, no opt-out information was linked to the user's Google account. Rather, users wishing to opt out needed to do so through the setting of an opt-out cookie on each of their devices. For opt-out cookies set in this way, there is no way of distinguishing one opt-out cookie from another: they would all have the generic value "OPT_OUT."

59. It is technically impossible to distinguish between Safari users who were affected by the issue at the heart of this action and those who were not.

60. For various reasons that I have described above, users in the following categories would not have received the DoubleClick Ad Cookie at all, or would not have received it as a result of the matters Plaintiffs complain about:

a. users who changed their default browser settings to reject all cookies;

b. users who had not updated their browser to a relevant version;

c. users who had not updated their operating system to a relevant version; and

d. users whose browsers did not interact with the DoubleClick domain.

Implications for Users Actually Affected

61. I will now seek to explain briefly the implications for users who received a DoubleClick Ad Cookie, regardless of the manner in which it was placed.

62. As I have indicated, users can control the information which the DoubleClick service uses to determine which advertisements to show. Users can (and could at all relevant times) opt out of receiving interest-based advertising altogether, or they can elect to choose topics in which they are interested, for example photography, or cycling, or cooking, in order to make the advertising they see more relevant to their interests. Depending on whether and how a user has chosen to manage their preferences, the DoubleClick service might seek to infer preferences like those I have mentioned.

63. The DoubleClick service does not (and did not at the relevant time) obtain and collate users' sensitive personal data in categories such as religious beliefs, racial or ethnic origin, health, sexuality, etc. Further, as a matter of practice, the DoubleClick service does not (and did not at the relevant time) permit advertisers to target any interest-based advertising on the basis of any sensitive characteristics, including religion, race, health or sexual orientation.

64. The only practical effect of having received the DoubleClick Ad Cookie, regardless of the manner in which the cookie is placed, is that a user may have seen interest-based advertising instead of the less-relevant contextual advertising that would otherwise have been seen. And some, if not most, users would likely have preferred interest-based advertising (and may have been unaware that Safari's default settings were marketed to prevent it). The presence of the DoubleClick Ad Cookie would not have increased the number of advertisements displayed to affected browsers / users. Even among those affected users who would have preferred not to receive interest-based advertising, it seems inevitable that their reactions (to the extent that they noticed at all) will have ranged from resigned indifference to mild irritation. Users who did notice the interest-based advertising and were offended by it could have opted out of interest-based advertising at any time.

65. In sum, for the reasons I have explained in this declaration, it is evident that the number of users actually affected by the issues complained of is proportionately small, and there is no means of differentiating them from a wider class of Safari users. I believe it is technically impossible to devise an approach whereby affected individuals could be differentiated from individuals who were not affected.

Internet Explorer

(During the relevant time period in 2011)

66. Plaintiffs also make allegations about Microsoft's Internet Explorer web browser ("IE"). IE handles cookies in a completely different way than Safari does. IE allows placement of the DoubleClick Ad Cookie in its default state. Microsoft purportedly designed IE's cookie handling behavior to rely on the "P3P" protocol under which a website is asked to send to the browser a copy of the website's privacy policy in a machine-readable P3P "Compact Policy Statement." Under the P3P protocol, if the terms used by a website in its statement are "unrecognized" by the browser, the browser should reject the unrecognized response, treat the website's privacy policy as "not present", and refuse to accept cookies.

67. Because the google.com website is unable to communicate its modern privacy policy in a P3P Compact Policy Statement, each time an IE browser requests such a statement from google.com, Google responds with the plain English message, "This is not a P3P policy!" and directs users to the full version of its privacy policy on its website. Despite the fact that the P3P protocol says this "unrecognized" response should be rejected, Microsoft nevertheless designed IE to accept the response and allow Google to place cookies on the browser.

68. The google.com domain does not place the DoubleClick Ad Cookie. Plaintiffs' allegations about IE thus have nothing to do with placement of the DoubleClick Ad Cookie that is the basis for Plaintiffs' claims.

Google's Statements About Cookies

69. I understand the Plaintiffs allege that Google has made certain statements about its privacy practices with respect to cookies. Specifically, Plaintiffs allege that Google's Privacy Policy stated: "Most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent." This is a true statement that warns that using a browser in its default state will likely result in the placement of cookies.

70. Plaintiffs also allege that Google's Help Center at one time stated that "Safari is set by default to block all third-party cookies." This out-of-date statement was posted to a rarely-visited Help Center page at a time when the statement was objectively true—long before the alleged conduct began and a year before Apple even implemented the exceptions to Safari's third-party cookie-blocking defaults that caused the placement of the DoubleClick Ad Cookie in the manner alleged by Plaintiffs.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this date: December 20, 2019

Lawrence You